Microsoft Azure

15MIN 雲端熱知識

Azure OpenAI 服務

怕資料外洩?
以 Azure OpenAI 打造具有企業級資安防護的 ChatGPT

Andy Li

台灣微軟 Microsoft Azure 資深雲端解決方案經理

Microsoft Azure

Agenda

- Azure OpenAI vs. OpenAI 有什麼差異
- 深入剖析企業常見的資安問題
- 如何打造具有企業等級安全防護的ChatGPT

OpenAI 專注於 AI 造福人類，而 Microsoft 旨在賦能每一個人與"組織"

	OpenAI	Microsoft
企業使命 Mission	確保通用人工智慧（AGI）造福**全人類**	賦能地球上的**每一個人**和**每一個組織**，都能實現更多、成就非凡
產品/服務 Product/Service	ChatGPT(Plus)	Azure ChatGPT API Teams Premium Bing Search/Image Creator Viva Sales Microsoft 365 Copilot Dynamics Copilot GitHub Copilot Microsoft Designer Microsoft Security Copilot
模型 Model	GPT X Codex Dall-E Embedding	GPT X Codex Dall-E Embedding
數位承諾 Privacy and Policy	不使用客戶透過 API 提交資料來訓練或改善模型 客戶透過 API 提交數據將保留最長 30 天，以防濫用和不當使用	+ (客戶有額外申請，可以不保留 30 天) 私有網路 (VNET) 資料傳輸 AD 整合存取權限 企業合規(SOC2、HIPAA、GDPR Data Privacy etc.) SLA 99.9%

+：與 OpenAI 相同

Why “Azure” OpenAI

Reliability & Scalability

- 多區域可用
- 保證SLA 99.9%
- 更高Rate Limit （TPM/QPM）
- 企業級有償Support

Management

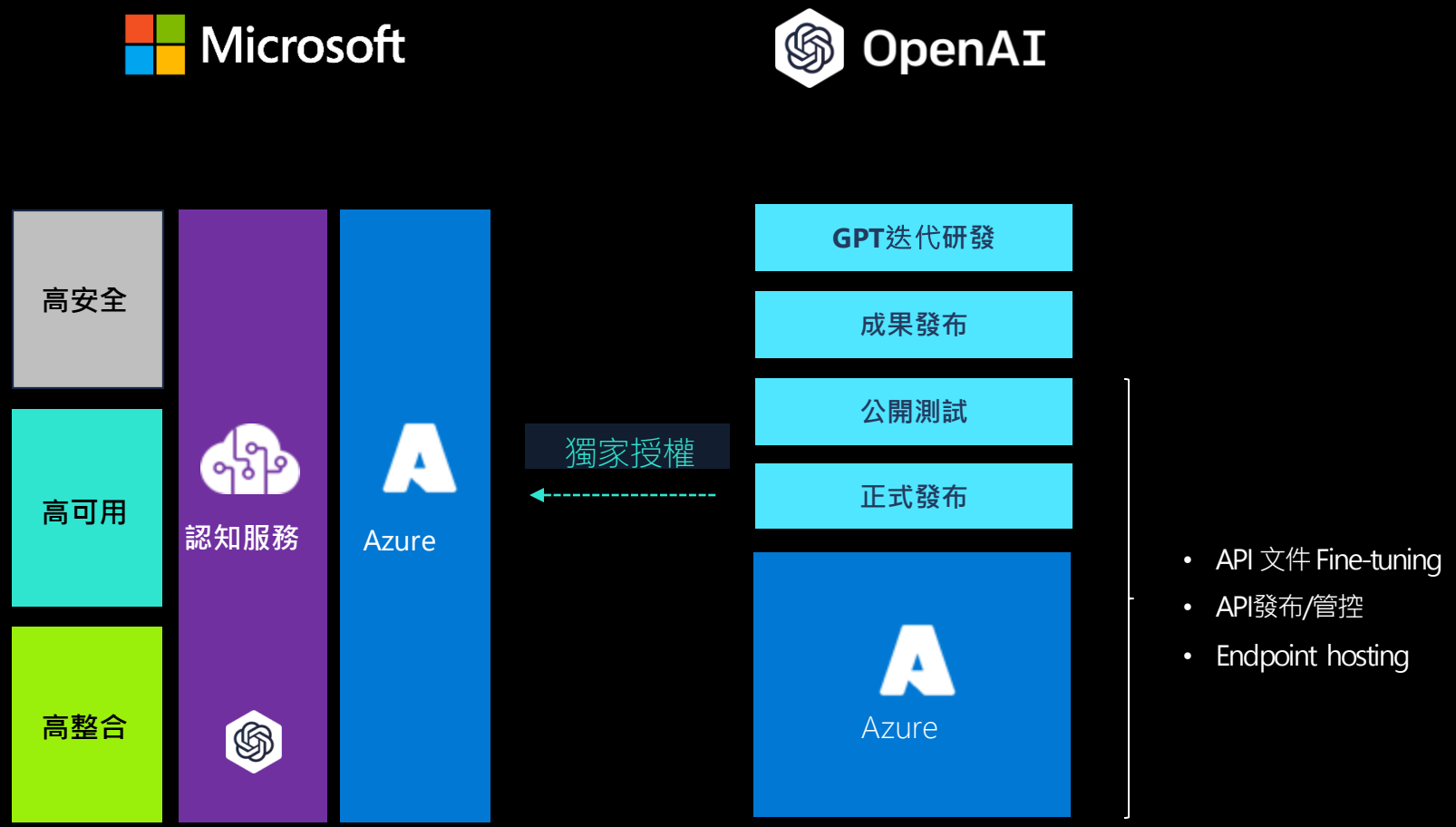
- Endpoint部署管理和監控
- Token監控
- 整合資源監控 （Monitor / Log Analytics）
- 更好的Error & debug支持

Extensibility

- Custom Domain
- 基於Azure的API擴充
- 整合現有Cognitive Service的服務架構
- 整合自動化 （Automation Task， ARM部署）

Security

- 企業合規 （SOC2， HIPAA， ISO， GDPR Data Privacy etc.）
- 私有網路（vNet）, Private Endpoint/Link
- 企業倫理審查 （Responsible AI）
- Azure AD 整合, RBAC/IAM 權限管理
- 托管身份 （Managed ID）



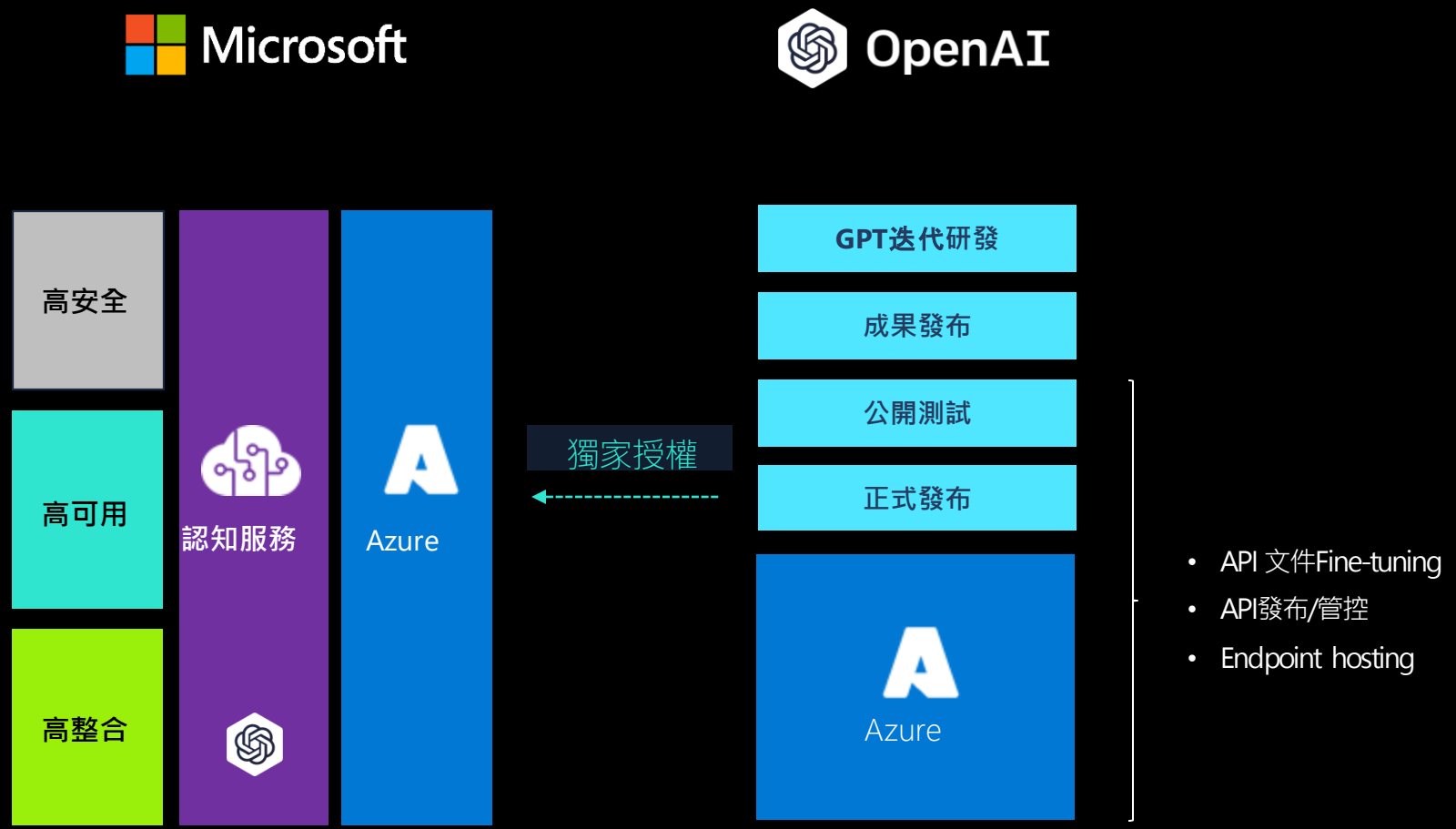
Why “Azure” OpenAI

Reliability & Scalability
- 多區域可用
- 保證SLA 99.9%
- 更高Rate Limit （TPM/QPM）
- 企業級有償Support

Management
- Endpoint部署管理和監控
- Token監控
- 整合資源監控 （Monitor / Log Analytics）
- 更好的Error & debug支持

Extensibility
- Custom Domain
- 基於Azure的API擴充
- 整合現有Cognitive Service的服務架構
- 整合自動化 （Automation Task， ARM部署）

Security
- 企業合規 （SOC2， HIPAA， ISO， GDPR Data Privacy etc.）
- 私有網路（vNet）, Private Endpoint/Link
- 企業倫理審查 （Responsible AI）
- Azure AD 整合, RBAC/IAM 權限管理
- 托管身份 （Managed ID）



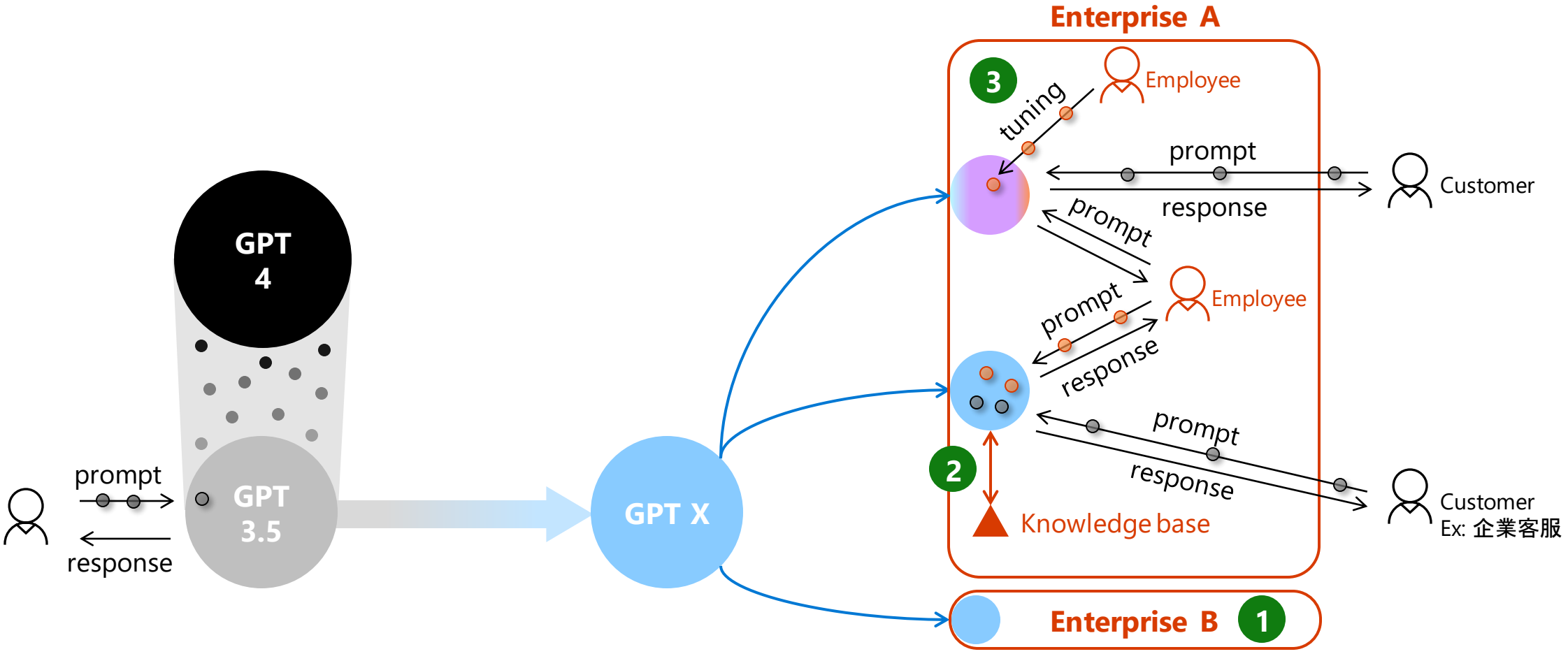
Microsoft Cloud
Runs on trust

Your data is your data
您的數據為你所有，微軟不會使用你的數據

Your data from any fine-tuning is not used to train the foundation AI models
你的數據不會被用來訓練微軟所提供給其他客戶的模型

Your data is protected by the most comprehensive enterprise compliance and security controls
你的數據將受到全方位的企業合規及安全措施的保護

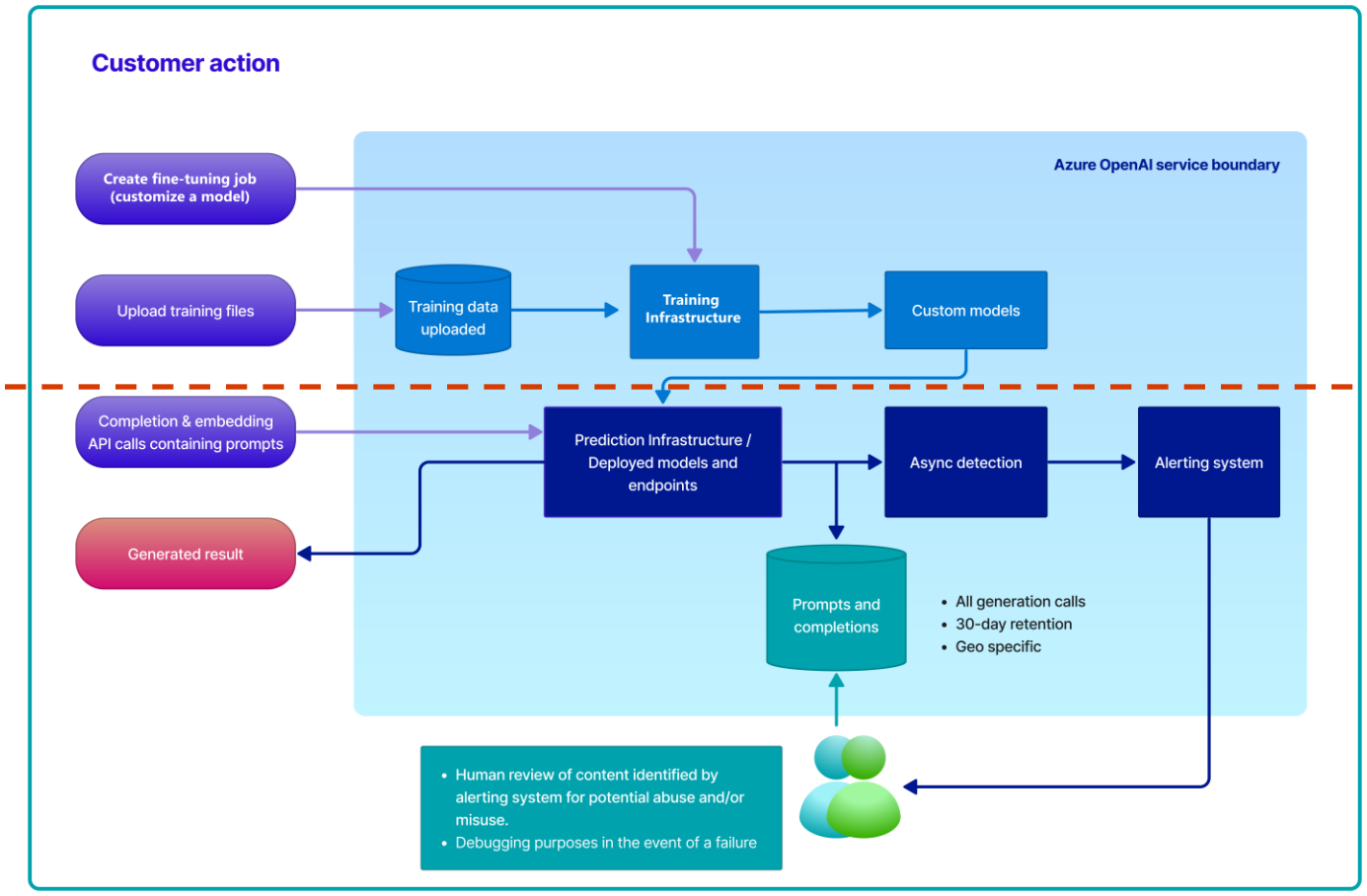
Azure OpenAI Service 為企業首選的生成式 AI 解決方案



1. 企業訂閱 Azure OpenAI 服務
2. GPT Model 結合企業內部知識庫
3. GPT Model Tuning 成企業自己的 GPT Model

資料的隱私和安全

Data, privacy, and security for Azure OpenAI Service



Finetune

Azure OpenAI 如何處理靜態資料的加密，特別是訓練資料和微調模型

- Encrypted and decrypted using FIPS 140-2 compliant 256-bit AES
- Microsoft-managed encryption keys (MMK)
- Customer-managed keys (CMK)
- Reference : Azure OpenAI Service encryption of data at rest

Microsoft 不會使用客戶資料來訓練或改進任何 Microsoft 的模型

- Reference : Training data for purposes of fine-tuning an OpenAI model

Inference

Azure OpenAI 服務可能會暫時儲存請求和回應資料，最長可達 30 天。

- Debugging purposes in the event of a failure
- Investigating patterns of abuse and misuse to determine if the service is being used in a manner that violates the applicable product terms.
- Reference : Preventing abuse and harmful content generation

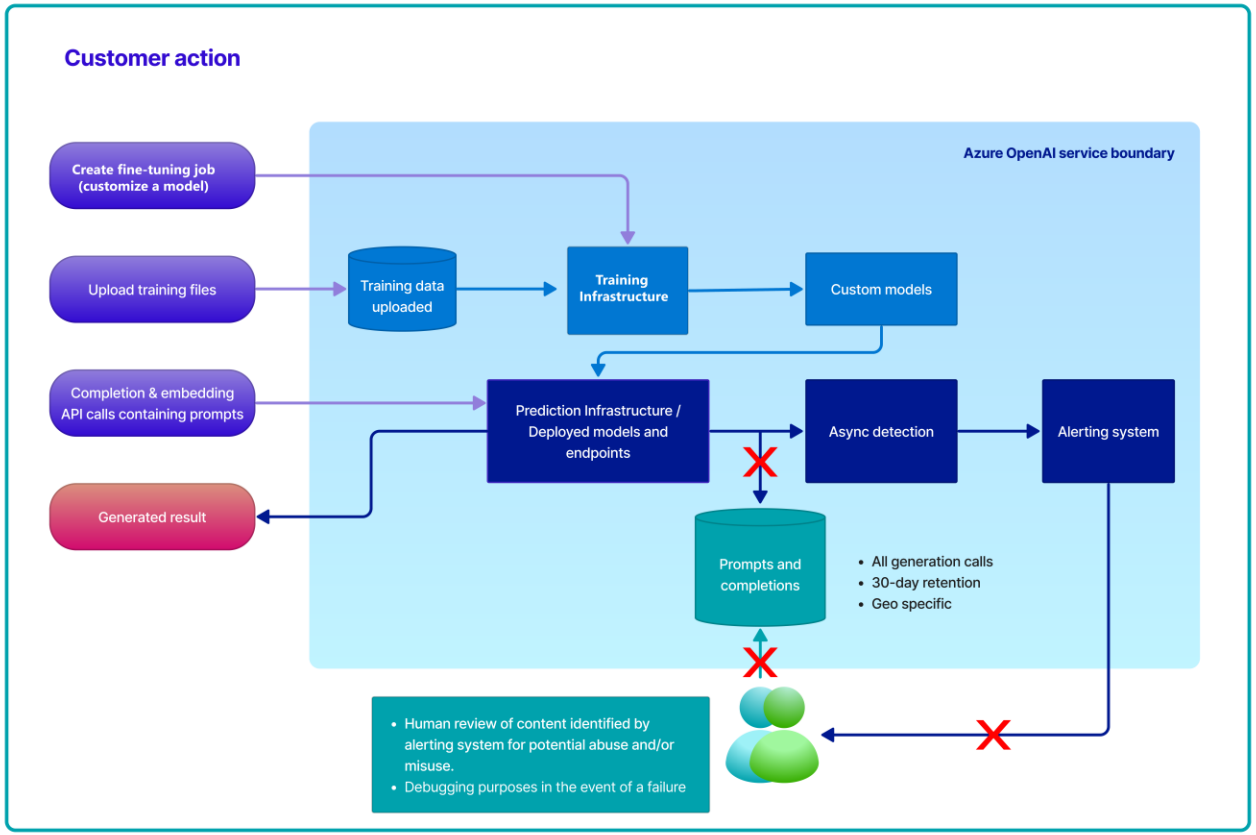
經授權的 Microsoft 員工可以查看觸發微軟自動化系統警告的prompt & completion data

- Reference : Abuse and harmful content generation

如何退出日誌紀錄和人工審核流程

Some customers may want to use the Azure OpenAI Service for a use case that involves the processing of sensitive, highly confidential, or legally-regulated input data but where the likelihood of harmful outputs and/or misuse is low. These customers may conclude that they do not want or do not have the right to permit Microsoft to process such data for abuse detection, as described above, due to their internal policies or applicable legal regulations. To address these concerns, Microsoft allows customers who meet additional Limited Access eligibility criteria and attest to specific use cases to apply to modify the Azure OpenAI content management features.

If Microsoft approves a customer's request to modify abuse monitoring, then Microsoft does not store any prompts and completions associated with the approved Azure subscription for which abuse monitoring is configured off. In this case, because no prompts and completions are stored at rest in the Service Results Store, the human review process is not possible and is not performed.



參考資料：[Can a customer opt out of the logging and human review process]

表單：https://aka.ms/oai/modifiedaccess

溫馨提醒

Availability | General Service Terms | **Service Specific Terms** | Add-ons | Related Resources

Azure OpenAI Service

In addition to the Limited Access Services terms above, the following terms apply to the use of the Azure OpenAI Service.

Use Limitations

- Microsoft may limit Customer's access to or use of Output Content or the Azure OpenAI Service if Microsoft has a reasonable basis to believe that the Output Content or Customer's use of the Azure OpenAI Service (i) violates the Acceptable Use Policy for Online Services; (ii) is inconsistent with the information submitted in connection with Customer's Limited Access Service registration form, or (iii) is inconsistent with requirements in the product documentation for the Azure OpenAI Service, as updated from time to time. "Output Content" means any data or content output by the Azure OpenAI Service.
- Customer may not use the Azure OpenAI Service to discover any underlying components of the models, algorithms, and systems, such as exfiltrating the weights of models.
- Customer may not use web scraping, web harvesting, or web data extraction methods to extract data from the Azure OpenAI Service or from Output Content.

Data Access and Use

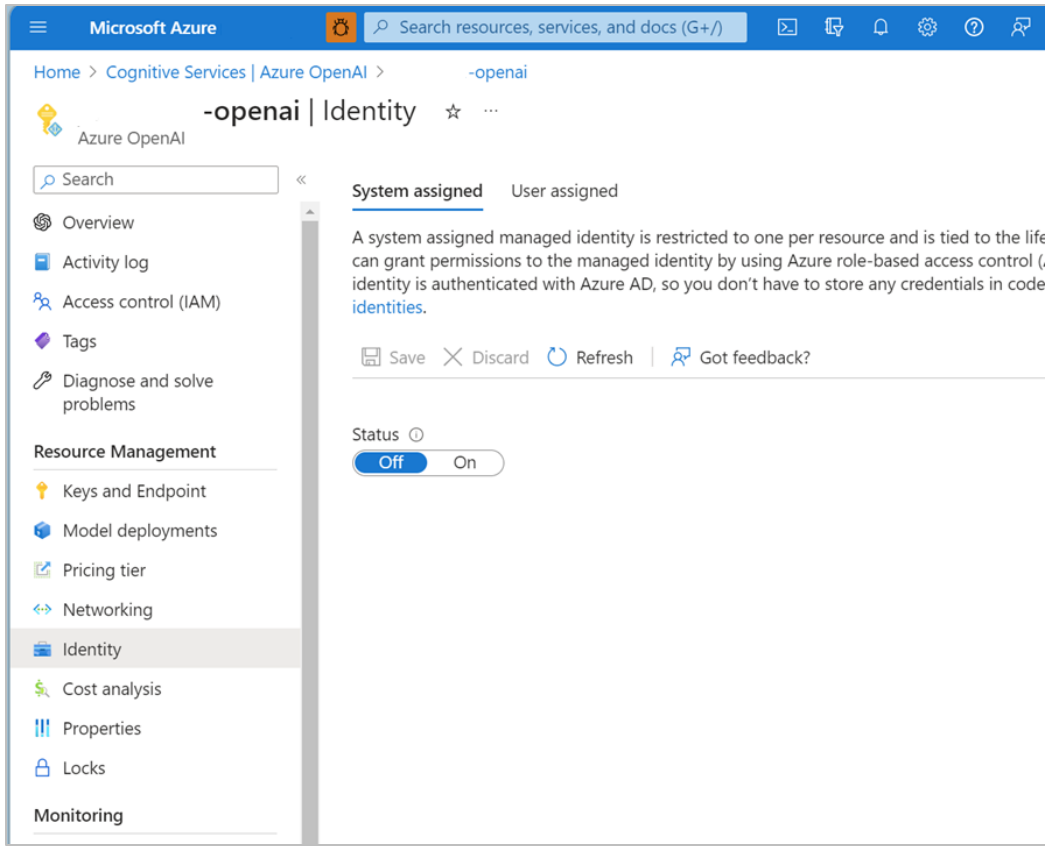
- Except as provided below, as part of providing the Azure OpenAI service, Microsoft will process and store **Customer Data** submitted to the service, as well as Output Content, for purposes of (1) monitoring for and preventing abusive or harmful uses or outputs of the service; and (2) developing, testing, and improving capabilities designed to prevent abusive use of and/or harmful outputs from the service. Authorized Microsoft employees may review data that has triggered our automated systems to investigate and verify potential abuse. Authorized Microsoft employees may also access and use this data to improve our systems that monitor for and prevent abusive or harmful uses or outputs of the service. In both cases, for customers who have deployed Azure OpenAI service in the European Economic Area, the authorized Microsoft employees will be located in the European Economic Area. See the Azure OpenAI product documentation https://learn.microsoft.com/azure/cognitive-services/openai/ for more information.
- The foregoing **Customer Data** processing terms will not apply if and to the extent Customer is approved for and complies with all requirements to use the Azure OpenAI service with Modified Content Filtering and/or Abuse Monitoring

Third Party Claims: Customer is responsible for responding to any third-party claims regarding Customer's use of the Azure OpenAI Service in compliance with applicable laws (including, but not limited to, copyright infringement or other claims relating to Output Content output during Customer's use of the Azure OpenAI Service).

Reference : Microsoft Product Terms

Managed Identity for Azure Resources

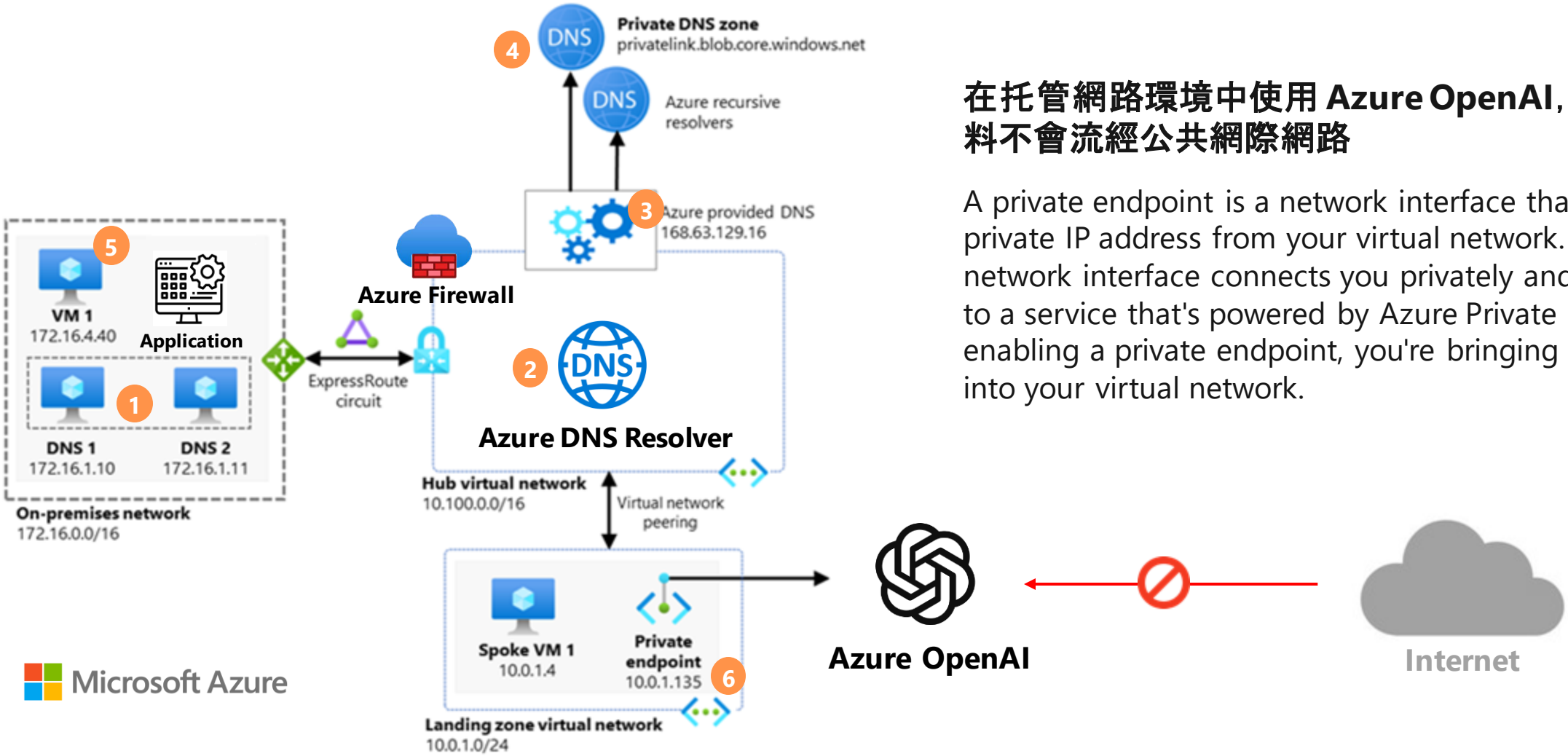
在 Azure Active Directory 中為應用程式提供自動受控識別(Managed Identity)，以便在連線至支援 Azure AD 驗證的資源時使用。應用程式可以使用受控身分識別來取得 Azure AD 權杖，而不需要管理任何認證。



- Service Principal Type = Managed Identity
- Locked down to only be modified by our service
- Can only be used on resources where it has been assigned (certificate)
- Key rotation managed by Azure

Reference : How to Configure Azure OpenAI Service with Managed Identities - Azure OpenAI

企業自有資料中心的延伸



在托管網路環境中使用 Azure OpenAI，所有的資料不會流經公共網際網路

A private endpoint is a network interface that uses a private IP address from your virtual network. This network interface connects you privately and securely to a service that's powered by Azure Private Link. By enabling a private endpoint, you're bringing the service into your virtual network.

打造具有企業級資安防護的 ChatGPT

iThome

新聞

員工外洩內部機密！[redacted]開放ChatGPT後出事緊急限縮使用

The Register、Tom's Hardware等媒體引述南韓當地媒體Economist的消息，指出[redacted]員工在不清楚ChatGPT使用規範下，為了工作之便直接將半導體設備、程式碼相關資訊上傳給ChatGPT進行處理，導致[redacted]的內部機密資料外洩

文/ 林妍溱 | 2023-04-07 發表

讚 197 分享

[redacted]的資料外洩事件是由南韓媒體《Economist》首先報導，Economist宣稱[redacted]員工逕自將公司機密資訊輸入ChatGPT，導致該公司半導體設備以及內部會議等資料外洩。（圖片來源[redacted]）

參考資料：員工外洩內部機密！[redacted]開放ChatGPT後出事緊急限縮使用 | iThome

南韓媒體《Economist》報導，南韓科技巨擘員工疑似因使用AI聊天機器人ChatGPT，而分別在不同事件中洩露公司機密。

報導指出，該公司裝置解決方案及半導體業務部門發生三起事件，出自員工將公司機密資訊輸入ChatGPT而外流。外洩的資訊包括半導體設備量測資料庫、生產／瑕疵設備相關軟體，以及一份公司會議語音轉錄的文字紀錄摘要。報導指出，一名軟體開發工程師在資料庫程式開發期間發現程式碼錯誤，於是將整份程式碼複製貼到ChatGPT對話中，以尋找臭蟲及解決方案。

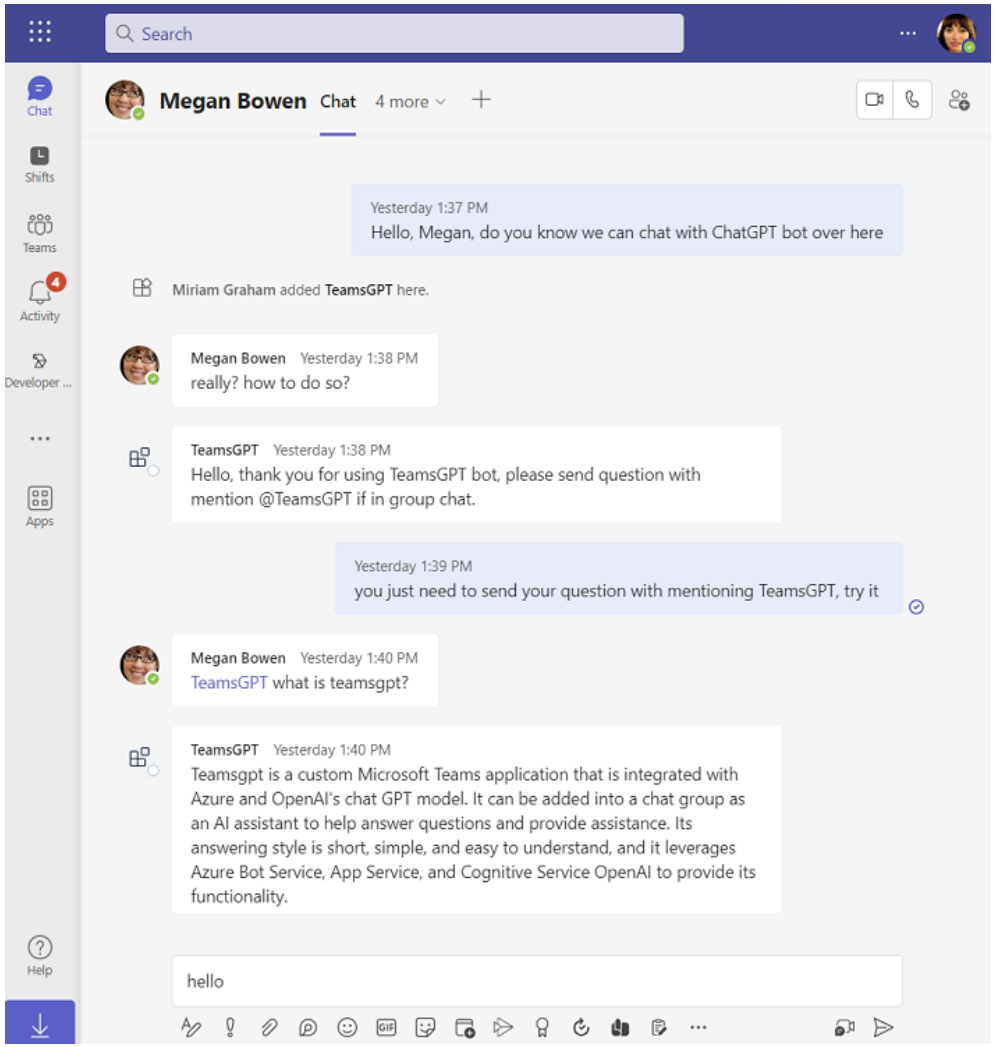
該公司原本因資訊安全禁止員工使用ChatGPT，該公司考慮開發可被公司監管的自有AI聊天機器人服務，3月11日才在員工要求下解除禁令，但該公司仍呼籲員工不得分享機密資訊。

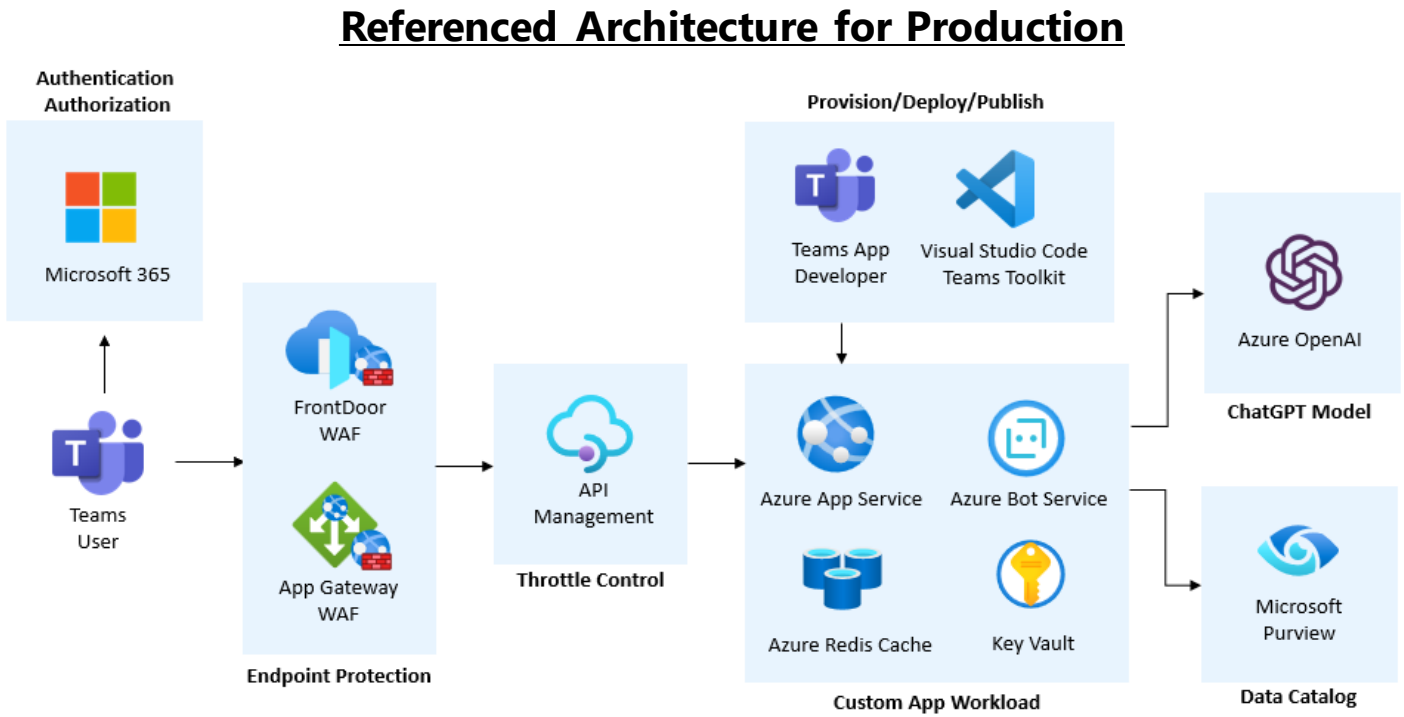
這起事件可能讓外部用戶透過詢問ChatGPT而得知該公司機密。報導指出，該公司緊急啟動資訊保護指施，將輸入ChatGPT的資訊量限制在每個問題1024 byte以下，並展開內部調查。該公司並警告員工，未來若再有類似事件將不再允許公司內部網路使用ChatGPT。

OpenAI也曾在公司FAQ網頁告誡用戶，不應在ChatGPT對話中分享敏感資訊。這些被上傳至ChatGPT的資訊，會被當成聊天機器人AI模型的訓練資料。

Microsoft Teams + Azure OpenAI + Microsoft Azure Networking/Security = **Secured Enterprise ChatGPT**

打造具有企業級資安防護的 ChatGPT





參考資料：[GitHub - Template project for integrating ChatGPT with Microsoft Teams]

Microsoft Azure

15MIN 雲端熱知識

持續鎖定 Microsoft Taiwan 與 Microsoft Azure Taiwan 臉書粉專

YouTube 資訊欄獲取更多相關資訊，講座簡報也可於資訊欄中取得

任何與 Azure 相關問題歡迎留言告訴我們！